# Most Active Band (MAB) Attack and Countermeasures in a Cognitive Radio Network

Nansai Hu, *Student Member, IEEE,* Yu-Dong Yao, *Fellow, IEEE,* and Joseph Mitola, *Fellow, IEEE*

***Abstract*—This paper investigates a type of attacks on a cognitive radio (CR) network, most active band (MAB) attack, where an attacker or a malicious CR node senses/determines the most active band within a multi-band CR network and targets this band through a denial of service (DoS) attack. We propose a countermeasure strategy, coordinated concealment strategy (CCS), to counter the MAB attack. Our results show that CCS significantly outperforms CR's inherent capability of signal/interference avoidance under a MAB attack. We also introduce power control in CCS to further improve the countermeasure performance in terms of the percentage of survival nodes.**

***Index Terms*—Cognitive radio, denial of service attack, most active band attack, cognitive interference.**

## I. Introduction

COGNITIVE radio (CR) offers great potentials for adaptive networks and dynamic spectrum access for enhanced spectrum utilization [1]. However, there are security vulnerabilities in CR networks. In the physical layer, a secondary or CR node first senses the channel environment to determine spectrum holes, which is subject to attack with an attacker manipulating the network environment. In access behavior or a medium access control (MAC) layer, misuse (e.g., misbehavior CR, selfish CR or cheating CR [2]) could occur due to the flexible or open access mechanisms in CR networks. In [2] to [5], behavior and MAC layer threats are considered in investigating CR network security. For CR physical layer threats, various attacks including DoS attacks and countermeasures have also been investigated in [6-13]. [6] discusses the issue of attacks due to CR malfunctions or misconfigurations (e.g., operation policies modified by attackers). Attacks from a malicious agent are investigated in [7]. Attacks can occur due to selfish behaviors of some CR nodes for unfair advantages in using spectrum [8]. It is also noted that the vulnerability of CR networks can be due to the fact that even weak attack signal levels could significantly disrupt a CR network [9] as spectrum sensing (low signal level detection) is an essential part of CR operations. DoS attacks and countermeasures in multi-channel CR networks have been reported in [10]. Frequency hopping based countermeasure techniques have been also studied [11], [12]. In fact, CR has its inherent signal/interference avoidance capabilities through its spectrum sensing function. Finally, while security strategies or a security sub-layer is introduced in a wireless standard [9], it is still unable to address the DoS security threats [13].

In this paper, we examine a type of DoS attacks and evaluate its impacts considering a multi-band CR network. In this attack, a malicious CR node or agent senses and monitors the signal activities over each band (e.g., spectrum sensing through energy detection) and then, attacks (with intentional interference) the band which has the most signal activities (e.g., the highest energy level) to achieve its maximum attack outcome. The band under attack could have either primary or secondary users. We refer this as the most active band (MAB) attack. We further introduce a countermeasure method against the MAB attack, known as coordinated concealment strategy (CCS). Our results show that CCS outperforms the CR signal avoidance feature/technique. We also consider the power control capability in CR nodes to achieve improved CCS countermeasure performance. Notice that such a MAB attack scenario could occur in a public service radio network with both legacy nodes (e.g., primary nodes) and cognitive radio nodes, where a malicious agent or node exploits the spectrum sensing and cognitive engine capabilities to launch most effective DoS attacks. It is therefore important to explore and develop potential MAB attack countermeasures.

The rest of this paper is organized as follows. Section II presents the MAB attack in a cognitive radio network. The coordinated concealment strategy is introduced in Section III and its performance results are presented in Section IV. Conclusions are drawn in Section V.

## II. Most Active Band Attack

### A. *Most Active Band Attack*

We consider $N_P$ primary nodes and $N_S$ secondary nodes (CR nodes) operating in a $M$-band CR network. In each band, $C$ is specified as the maximum user or node capacity, implying that the maximum number of nodes which can be allocated within a band is $C$. We assume that feature detection based spectrum sensing is implemented in each secondary node so that all the secondary nodes avoid bands with primary nodes. The number of bands with primary nodes (primary bands) is assumed to be $M_P$ and the number of vacant bands (secondary bands) is assumed to be $M_S$ ($M_P + M_S = M$). We consider a denial of service (DoS) based attack and an attacker or a malicious CR node emits intentional interference on one or several bands and denies the services in those bands. To maximize its impact, the malicious node targets/attacks the band(s) with the most signal activities (energy levels). In this

Manuscript received May 17, 2011; revised July 5, 2011 and November 15, 2011; accepted December 18, 2011. The associate editor coordinating the review of this paper and approving it for publication was C. Cordeiro.

N. Hu and Y.-D. Yao are with the Electrical and Computer Engineering Department, Stevens Institute of Technology, Hoboken, NJ 07030, USA (e-mail: {nhu1, yu-dong.yao}@stevens.edu).

J. Mitola is with the School of Systems & Enterprises and the School of Engineering & Science, Stevens Institute of Technology, Hoboken, NJ 07030, USA (e-mail: joe.mitola@stevens.edu).

Digital Object Identifier 10.1109/TWC.2012.011812.110927

paper, we consider a scenario in which the malicious node attacks one band at a time and it is referred to as a most active band attack. This can also be seen as a type of cognitive interference which has the spectrum sensing (energy detection) and cognitive engine capabilities to determine the band with the most signal activities. The following equation describes the band (band $i^*$) a MAB attacker (a malicious CR node) selects to target,

$$i^* = \{i \mid \max_{i\in\{1,2,\ldots,M\}} (\sum_{j=1}^{N_S} |h_j|^2 x_{ij} + \sum_{k=1}^{N_P} |h_k|^2 x_{ik})\} \tag{1}$$

where

$$\sum_{i=1}^{M_S} x_{ij} = 1 \ \ , \ \ \sum_{i=1}^{M_P} x_{ij} = 0 \tag{2}$$

$$\sum_{i=1}^{M_P} x_{ik} = 1 \tag{3}$$

and $x_{ij} \in \{0,1\}$, $x_{ik} \in \{0,1\}$. $x_{ij} = 1$ indicates that secondary node $j$ operates in band $i$ and $x_{ij} = 0$ indicates otherwise. $|h_j|$ represents the channel gain between the attacker and node $j$. Similarly, $x_{ik} = 1$ indicates that primary node $k$ operates in band $i$ and $x_{ik} = 0$ indicates otherwise. $|h_k|$ represents the channel gain between the attacker and node $k$. As described in Eq. (1), the MAB attacker targets the most active band ($i^*$) among all $M$ bands through energy level comparisons. Eq. (2) specifies that a secondary node operates in one secondary band only and does not interfere with primary bands. Eq. (3) denotes that a primary node operates in one primary band only. Furthermore, the following equation specifies the node capacity consideration in each band,

$$\sum_{j=1}^{N_S} x_{ij} \leq C \ , \ \sum_{k=1}^{N_P} x_{ik} \leq C \tag{4}$$

### *B. Impacts of Most Active Band Attack*

As a DoS based attack, a MAB attacker could potentially target either a secondary band or a primary band depending on primary/secondary user activity levels. When a MAB attacker targets one primary band, the primary nodes under attack are unable to avoid the attacker since they have no spectrum sensing and reconfiguration capabilities. When a MAB attacker targets one secondary band, the secondary nodes under attack could hop to other bands to avoid the attacker. However, the MAB attacker could follow the secondary nodes due to its energy detection (spectrum sensing) capabilities. Therefore, this CR's inherent signal/interference avoidance capability is no longer effective in countering a MAB attack. During the process of signal/interference avoidance (band change), significant amount of control signaling occurs (e.g., request, acknowledgement and channel setup, etc.), which reduces communication efficiency and introduces extra synchronization complexity. The conventional frequency hopping [11], [12] based methods (e.g., band hopping) are also no longer effective, since the MAB attacker can follow the CR to its new operating band. Notice that the MAB attack is a realistic and significant threat. First, with its cognitive capability, a MAB attacker is able to launch targeted attacks. Second, its impact can be substantial as CR's inherent interference avoidance capabilities or existing anti-attack methods are no longer effective in countering MAB attacks.

For performance evaluations under MAB attacks, we calculate the number of surviving nodes (e.g., nodes which are not in a targeted band) over the total number of nodes. We use $A^S_{i,i^*}(j)$ and $A^P_{i,i^*}(k)$ to denote that whether a secondary/primary node is under attack, respectively.

$$A^S_{i,i^*}(j) = \begin{cases} 1, & x_{ij} = 1 \cap i = i^* \\ 0, & \text{otherwise} \end{cases} \tag{5}$$

$$A^P_{i,i^*}(k) = \begin{cases} 1, & x_{ik} = 1 \cap i = i^* \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

The percentage of surviving secondary nodes and primary nodes, $V_S$ and $V_P$, can be obtained by $V_S = (\sum_{j=1}^{N_S}(1 - A^S_{i,i^*}(j)))/N_S$ and $V_P = (\sum_{k=1}^{N_P}(1 - A^P_{i,i^*}(k)))/N_P$ respectively. Further, the percentage of the total surviving nodes in the network, $V$, can be obtained by

$$V = \frac{\sum_{j=1}^{N_S}(1 - A^S_{i,i^*}(j)) + \sum_{j=1}^{N_P}(1 - A^P_{i,i^*}(k))}{N_S + N_P} \tag{7}$$

Notice that only active primary nodes and active secondary nodes are considered in the network model and in the performance metric (Eq. (5), (6), and (7)).

## III. MAB Attack Countermeasures

In this section, we introduce a MAB countermeasure, known as the coordinated concealment strategy. The objective of CCS is to minimize the number of nodes in the targeted band, which maximizes the number of surviving nodes. In the presence of a MAB attacker, in CCS, a few secondary nodes converge to a single band to create a most active band (e.g., highest energy level). This band will be attacked by the malicious CR node (a MAB attacker) and those secondary nodes will be sacrificing nodes. All remaining secondary nodes and all primary nodes will operate in other bands and will be surviving nodes. It is seen that the basic idea of the CCS algorithm is to use the sacrificing nodes as a cover to conceal the signal activities of the surviving nodes. In the CCS process, due to the channel gain variability ($|h_j|$ and $|h_k|$ in Eq. (1)) of each node, different nodes have different contributions to the energy level in each band (signal activities seen by the MAB attacker). The CCS algorithm or the selection of the sacrificing nodes are described as follows.

$$\max(V_S) \quad \equiv \quad \min_{A^S_{i,i^*}(j)} \sum_{j=1}^{N_S} x_{i^*j} \tag{8}$$

$$\text{s.t.} \qquad \sum_{k=1}^{N_P} x_{i^*k} = 0 \tag{9}$$

$$\sum_{j=1}^{N_S} |h_j|^2 x_{i^*j} + \sum_{k=1}^{N_P} |h_k|^2 x_{i^*k} \geq \sum_{j=1}^{N_S} |h_j|^2 x_{ij} + \sum_{j=1}^{N_P} |h_k|^2 x_{ik} \tag{10}$$
$$\forall i \in \{1,2,...,M\}$$

$$\sum_{i=1}^{M_S} x_{ij} = 1 \ \ , \ \ \sum_{i=1}^{M_P} x_{ij} = 0 \tag{11}$$

$$\sum_{k=1}^{M_P} x_{ik} = 1 \tag{12}$$

$$\sum_{j=1}^{N_S} x_{ij} \leq C\ ,\ \sum_{k=1}^{N_P} x_{ik} \leq C \tag{13}$$

In Eq. (8), the objective is to maximize the system performance metric $V_S$. This is equivalent to minimizing the number of nodes in the targeted band ($A_{i,i^*}^S(j)$ as in Eq. (5)). This objective is subject to protecting all primary nodes from a MAB attack (Eq. (9)). Eq. (10) denotes that the energy level (signal activity) of the targeted band is greater than that of other bands. Eq. (11) and Eq. (12) specify that each secondary node operates in one secondary band only and each primary node operates in one primary band only. Eq. (13) defines the node capacity in each band. For channel gains, $|h_j|$ and $|h_k|$, we consider the impact of both a path loss exponent and channel fading attenuations. We denote $r_j$ as the distance between a secondary node $j$ to the MAB attacker and $r_k$ as the distance between a primary node $k$ to the MAB attacker. We assume that $r_j$ and $r_k$ follow the distributions bellow [14],

$$\Pr(r_j) = \begin{cases} \frac{2r_j}{R^2 - R_0^2}, & r_j \in [R_0, R] \\ 0, & \text{otherwise} \end{cases} \tag{14}$$

$$\Pr(r_k) = \begin{cases} \frac{2r_k}{R^2 - R_0^2}, & r_k \in [R_0, R] \\ 0, & \text{otherwise} \end{cases} \tag{15}$$

With the MAB attacker being in the center and $R$ being the radius of a circular grid of a CR network, which includes all the nodes and the attacker. Also, there is no node presence within a radius $R_0$ around the center (attacker). In implementing CCS, the distances between nodes and the attacker ($r_j$ and $r_k$) can be estimated based on signal strength information [15], [16]. Notice that radio localization (attacker localization) plays an important role in CCS implementation and some related studies of attacker localization have been reported in [5] and [17]. A central agency or node can be used to collect the signal strength information and perform optimizations in determining sacrificing nodes and, if power control is implemented, required transmit power levels. Also notice that we consider symmetric channels (forward/reverse links) and the CR-attacker link strength information is obtained based on the attacker-CR link information.

As described in the CCS algorithm, the channel gains and node distributions play important roles in determining the CCS performance. Our objective is to maximize the number of surviving nodes. The CCS algorithm as defined in (8) through (13) can be further improved by incorporating power control in the secondary nodes. This is to increase the transmission power levels of some secondary nodes, thus reducing the number of sacrificing nodes needed in CCS. The CCS algorithm with power control can be defined using (8) through (13), substituting (10) with

$$\sum_{j=1}^{N_S} |h_j|^2 x_{i^*jP_j} + \sum_{k=1}^{N_P} |h_k|^2 x_{i^*k} \geq \sum_{j=1}^{N_S} |h_j|^2 x_{ijP_j} + \sum_{j=1}^{N_P} |h_k|^2 x_{ik}$$
$$\forall i \in \{1, 2, ..., M\} \tag{16}$$

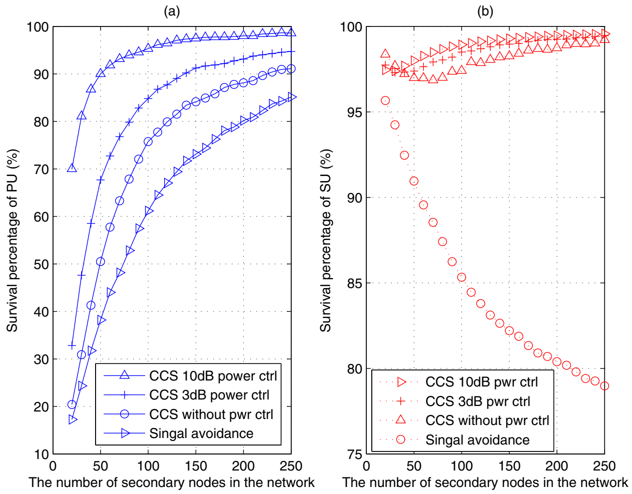

Fig. 1. (a) Survival percentage of primary nodes; (b) Survival percentage of secondary nodes. The number of frequency bands $M = 6$; Total 50 primary nodes are in one band; Maximum node capacity of each band $C = 50$.

In addition, we have the following constrains in implementing the power control.

$$P_L \leq \forall P_j \leq P_U \tag{17}$$

$$\sum_{j=1}^{N_S} P_j = N_S \tag{18}$$

where $P_j$ presents the transmit power of secondary node $j$. In Eq. (16), we consider $P_j$ when calculating the energy level (signal activity) of each band. Eq. (17) specifies the power control range of a secondary node, considering an allowed maximum power level ($P_U$) and a minimum power ($P_L$). The minimum power level is specified to satisfy a transmission performance requirement. The total transmit power in the network (all secondary nodes) is assumed to be a constant (Eq. (18)).

## IV. Simulation Results

In this section, we present the countermeasure performance of the proposed CCS methods. The results are obtained using Matlab simulation. The geographical locations of primary and second nodes are determined following Eq. (14) and (15) with $R = 1000$ m and $R_0 = 10$ m. We place an attacker in the center of a simulated network, considering a six-band CR network ($M = 6$) where 50 primary nodes ($N_P = 50$) are operating within one band ($M_P = 1$). The capacity of each band, $C$, is assumed to be 50. The number of secondary nodes ($N_S$) varies from 20 to 250. The channel gain is assumed to include a path loss with exponent of 3 with Raleigh fading. Notice that there are several essential elements in a CR network, including the dynamics of primary users (on/off or presence/absence) and a spectrum sensing process. This paper investigates DoS attack countermeasures or strategies after successful spectrum sensing or primary user determinations (identifications of channels occupied by primary nodes). In Fig. 1, we investigate the countermeasure performance considering different network sizes (the number of secondary nodes)

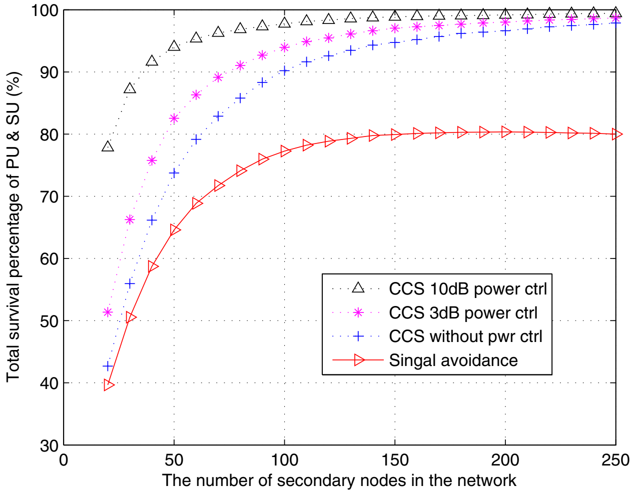

Fig. 2. Survival percentage of all nodes. The number of frequency bands $M = 6$; Total 50 primary nodes are in one band; Maximum node capacity of each band $C = 50$.

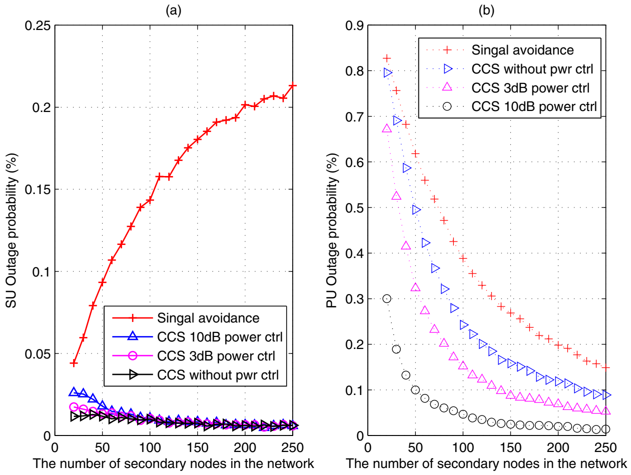

Fig. 3. (a) Outage percentage of secondary nodes; (b) Outage percentage of primary nodes. The number of frequency bands $M = 6$; Total 50 primary nodes are in one band; Maximum node capacity of each band $C = 50$.

and present the survival percentage of primary nodes and second nodes respectively. Four curves are plotted in Fig. 1(a), which correspond to a conventional CR network (with signal avoidance features), a CR network with CCS, a CR network with CCS and power control (3 dB power range), and a CR network with CCS and power control (10 dB power range). Fig. 1(a) shows the survival percentage of primary nodes, which indicates that a significant performance improvement is achieved with CCS as compared to the conventional CR signal avoidance capabilities. Further performance improvement can be obtained with power control in CCS. As illustrated in the figure, when $N_S = 100$, the primary node survival percentage increases from approximately 60% (signal avoidance), 75% (CCS), 85% (CCS with 3 dB power control), to 95% (CCS with 10 dB power control).

Fig. 1(b) shows the survival percentage of secondary nodes and the performance changes significantly when the network size varies. When the network size is small (smaller $N_S$), the primary band is the most active band and it is under attack, which leads to a high secondary node survival percentage. When the number of secondary nodes increases, there are enough secondary nodes to conceal the primary nodes and the secondary nodes survival percentage becomes low. Further increases of secondary nodes improve the secondary nodes survival percentage as many secondary nodes are concealed by some sacrificing secondary nodes. It is important to notice that, as shown in Fig. 2, the total survival percentage of primary nodes and secondary nodes improves consistently with CCS and CCS plus power control. When $N_S = 250$, the total primary node and secondary node survival percentage improves from approximately 80% (signal avoidance), 95% (CCS), 97% (CCS with 3 dB power control), to 99% (CCS with 10 dB power control).

We consider a cooperative CR network in which, at a given time, there will be some sacrificing nodes in order to protect survival nodes. Due to the nature of random distributions and movement of SUs and the effect of channel fading, a SU node can be "randomly" selected as a sacrificing node (following a network optimization process). This, to a certain extend, inherently addresses the issue of fairness among all SUs. Notice that a SU node's status as a sacrificing or survival node also changes with time, which effectively relates to the SU outage probability, as shown in Fig. 3(a), due to being a sacrificing node. The primary node performance in terms of the outage probability is shown in Fig. 3(b), which illustrate the performance improvement due to CCS and power control.

## V. Conclusion

In this paper, we introduce a MAB attack and investigate its impacts on a CR network. We then proposed a MAB attack countermeasure, CCS. Numerical results show that CCS outperforms CR's inherent signal/interference avoidance feature. Furthermore, power control is incorporated in the CCS method to enhance the MAB countermeasure performance.

## References

[1] J. Mitola and G. Maguire, "Cognitive radio: making software radios more personal," *IEEE Personal Commun.*, vol. 6, 1999.

[2] S. Arkoulis, L. Kazatzopoulos, C. Delakouridis, and G. F. Marias, "Cognitive spectrum and its security issue," *2008 International Conference on Next Generation Mobile Applications, Services and Technologies*.

[3] J. L. Burbank, "Security in cognitive radio network: the required evolution in approaches to the wireless network security," *2009 International Conference on Cognitive Radio Oriented Wireless Networks and Communications*.

[4] T. C. Clancy and N. Goergen, "Security in cognitive radio network: threat and mitigation," *2008 International Conference on Cognitive Radio Oriented Wireless Networks and Communications*.

[5] R. Chen, J. M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. Sel. Areas Commun.*, vol. 26, pp. 25–37, 2008.

[6] Y. Zhang, G. Xu, and X. Geng, "Security threats in cognitive radio networks," *2008 IEEE International Conference on High Performance Computing and Communications*.

[7] T. X. Brown and A. Sethi, "Potential cognitive radio denial of service attacks and remedies," *2007 International Symposium on Advanced Radio Technologies*.

[8] W. Wang, "Denial of service attacks in cognitive radio networks," *2010 International Conference on Environmental Science and Information Application Technology*.

[9] C. Cordeiro, K. Challapali, D. Birru, and N. S. Shankar, “IEEE 802.22: the first worldwide wireless standard based on cognitive radios,” *2005 IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks*.

[10] H. Li and Z. Han, “Dogfight in spectrum: jamming and anti-jamming in multichannel cognitive radio systems,” *2009 IEEE Global Telecommunications Conference*.

[11] L. Wang and Y. Wang, “Method for security enhancement of cognitive radio system,” *2009 International Symposium on Intelligent Ubiquitous Computing and Education*.

[12] J. Ma, Y. Zhong, and S. Zhang, “Frequency-hopping based secure schemes in sensornets,” *2005 International Conference on Computer and Information Technology*.

[13] K. Bian and J.-M. Park, “Security vulnerabilities in IEEE 802.22,” *2008 International Wireless Internet Conference*.

[14] Z. Jin, S. Anand, and K. Subbalakshmi, “Mitigating primary user emulation attacks in dynamic spectrum access networks using hypothesis testing,” *ACM Mobile Computing and Commun. Rev.*, vol. 13, 2009.

[15] K. Whitehouse, C. Karlof, and D. Culler, “A practical evaluation of radio signal strength for ranging-based localization,” *ACM Mobile Computing and Commun. Rev.*, vol. 11, 2007.

[16] N. Li and P. Li, “A range-free localization scheme in wireless sensor networks,” *2008 IEEE International Symposium on Knowledge Acquisition and Modeling Workshop*.

[17] Y. Chen, W. Trappe, and R. P. Martin, “Attack detection in wireless localization,” *2007 IEEE International Conference on Computer Communications*.